WHAT IS CLAIMED IS:

1. A basic input/output system (BIOS) update file comprising:

a signed data area including a volume header, signed data, and executable update code;

a signature; and

an unsigned data area including an update command list and unsigned data.

2. The BIOS update file of claim 1 further comprising a file header.

3. The BIOS update file of claim 2 in which the file header comprises data in conformance with an extensible firmware interface (EFI) specification.

4. The BIOS update file of claim 1 in which the volume header comprises a list representing locations of components within the BIOS update file.

5. The BIOS update file of claim 1 in which the signed data area comprises:

secure BIOS update data; and

an access control list representing permitted commands.

6. The BIOS update file of claim 1 in which the executable update code comprises code to enforce security rules regarding types of modifications permitted to the signed data area.

7. The BIOS update file of claim 1 in which the update command list comprises commands requested by an unauthenticated entity for modifications of the signed data.

8. A method comprising;

executing update code in a basic input/output system (BIOS) update file to modify data in an unsigned data portion and add commands relating to the data;

verifying a digital signature of the BIOS update file;

executing the update code for processing the commands in the unsigned data portion affecting data in a signed data portion; and

committing the BIOS update file.

9. The method of claim 8 in which the unsigned data portion comprises unauthenticated data.

10. The method of claim 8 in which verifying comprising aborting upon occurrence of verification failure.

11. The method of claim 8 in which executing the update code for processing the commands comprises:

verifying the commands against an access control list; and

in response to the verifying, modifying the signed data portion with the data in the unsigned data portion.

12. A computer program product, tangibly embodied in an information carrier, for updating a flash memory basic input/output system (BIOS), the computer program product being operable to cause data processing apparatus to:

execute update code in a BIOS update file to modify data in an unsigned data portion and add commands relating to the data;

verify a digital signature of the BIOS update file;

execute the update code for processing commands in the unsigned data portion affecting data in a signed data portion; and

commit the BIOS update file.

13. The product of claim 12 in which the unsigned data portion comprises unauthenticated data.

14. The product of claim 12 in which verifying comprises aborting upon occurrence of verification failure.

15. The product of claim 12 in which executing the update code for processing commands causes the data processing apparatus to:

verify the commands against an access control list; and

in response to the verifying, modify the signed data portion with the unsigned data portion.

16. A method comprising:

adding data to an unsigned data portion of a basic input/output system (BIOS) update file;

adding commands to the unsigned data portion of the BIOS update file;

verifying a signature in the BIOS update file with a signature residing in target hardware;

verifying the commands against an access control lost residing in a signed data portion of the BIOS update file; and

modifying data in the signed data portion of the BIOS update file with data in the unsigned portion in response to the commands.

17. The method of claim 16 in which the commands comprise:

a command to add data in the unsigned data portion to data in the signed data portion;

a command to modify data in the signed data portion with data in the unsigned data portion; and

a command to delete data in the signed data portion.

18. The method of claim 16 in which verifying the signature in the BIOS update file with the signature in the target hardware comprises a public key/private key encryption process.

19. The method of claim 18 in which the public key/private key encryption process is an RSA encryption process.

20. The method of claim 16 further comprising generating an image for the data in the signed data portion.

21. The method of claim 20 further comprising flashing the image into flash memory of target hardware.

22. The method of claim 21 in which the flash memory comprises flash memory modules.

23. A computer program product, tangibly embodied in an information carrier, the computer program product being operable to cause data processing apparatus to:

add data to an unsigned data portion of a basic input/output system (BIOS) update file;

add commands to the unsigned data portion;

verify a signature in the BIOS update file with a signature in target hardware;

verify the commands against an access control list (ACL) residing in a signed portion of the BIOS update file; and

modify data in the signed portion with data in the signed portion in response to the commands.

24. The product of claim 23 in which the commands comprise:

a command to add data from the unsigned data portion to data in the signed data portion;

a command to modify data in the signed data portion with data in the unsigned data portion; and

a command to delete data in the signed data portion.

25. The product of claim 23 further causing the processor to:

generate an image for the data in the signed data portion.

26. The product of claim 25 further causing the processor to:

flash the image into a flash memory pf the target hardware.

27. A system comprising:

a processor;

a memory including a basic input/output system (BIOS) installation process, and a flash memory containing a BIOS with digital signature verification;

a medium containing a BIOS update file, the BIOS update file comprising:

a signed data portion including a volume header, signed data and executable update code to configure the signed data with unsigned data in an unsigned data portion; and

a digital signature.

28. The system of claim 27 in which the BIOS update file further comprise:

an access control list having authorized commands in the signed data portion; and

a list of commands in unsigned data portion.

29. The system of claim 28 in which the authorized commands comprise commands to enforce security rules regarding types of modifications permitted to the signed data.